Minimum Security Baseline Home

Version Control

Version	Date	Change	Change made by
.001	12/1/2014	Updated downloadable version of the MSB and several sub-category definition reference numbers. Updated compensating control request FAQ.	Jenn Stewart
.002	2/26/2015	Moved frequently asked questions to a child page. Definition column moved inline with actual requirement. Links to Best Practice documents for categories added to Resources column.	Jenn Stewart
.003	3/3/2015	Re-linked several best practice documents so the appropriate category was matched with the corresponding best practice.	Jenn Stewart
.004	3/26/2015	Reference to SSL was removed from item 5.2.1 "Encrypted transmission means (e.g., TLS, SFTP, IPSec VPN) will be used wherever possible" due to the weaknesses within the protocol. Transport Layer Security (TSL) was added in place of SSL.	Jenn Stewart

Download the MSB.

PREFACE

In order for any institution to protect sensitive data, it must first define what sensitive data really is in the context of its industry and society. It must locate that data and then it must adequately protect it. For Penn State, the Data Categorization policy (AD71) defines three levels of categorization or “sensitivity” for data (public, internal/controlled and restricted). These in turn necessitate two levels of system and network protection (public and non-public (which includes both internal/controlled and restricted)). For examples of information in the three categories, users should see the Data Categorization policy (AD71) and Data Categorization Examples (ADG07) published separately from this document. The Minimum Security Baseline that must be implemented follow below. Security is a balancing act between the need to protect and the need for usability and openness. The Minimum Security Baseline strike that balance, knowing that even with that said there will be instances and implementations that can’t meet the exact “letter of the law”. In those cases, an exception process will be defined and published as a part of the implementation of the Baseline.

Penn State Minimum Security Baseline

The minimum security baseline applies in several dimensions. Primarily the baseline is geared to the categorization of the data (public, internal/controlled and restricted. The definitions of these terms are included in policy AD71). The categorization of the data then in turn drives both system and network architecture, which must be divided into two primary categories (public and non-public). The most restricted data may require additional controls, which are also listed below.

Note: Systems, networks and data may have additional integrity (accuracy) or availability requirements exceeding the basic categorization of the data processed, transmitted or stored therein. Availability and integrity needs must be considered when architecting a network and configuring systems that attach to the network. However, those requirements are separate from those associated with data sensitivity and are not included below.

Exceptions: In any Security Baseline, the need for exceptions exists. No one architecture will meet all operational requirements in all cases. Therefore, as stated previously, there will be exceptions required by individual units to some of the stated requirements. A process of identifying

compensating controls must begin in cases where a true need for an exception exists. When an exception is requested, ITS Security Operations and Services and local IT staff will work together with the user to find a solution that meets both the user's needs and the protection requirements necessary for institutional due diligence. In other words, The Security Baseline should not be viewed as having no alternatives. There are alternatives in some cases, but they must be carefully planned to fulfill the needs of all concerned while still meeting the legal and regulatory demands placed upon the institution.

If for any reason units cannot comply with a particular requirement, requests for exceptions should be sent to ITS Security Operations and Services (security@psu.edu). ITS SOS will coordinate with other offices (e.g., Privacy, Office of General Counsel, Internal Audit) as necessary.

Security Requirements

Primary Categories of Systems/Networks: Public, Non-Public

Primary Categories of Data: Public, Internal/Controlled, Restricted

NOTE: ALL LISTED SECURITY MEASURES ARE ALSO ENCOURAGED FOR PUBLIC DATA. WHERE X'S APPEAR IN THE TABLE, THE MEASURE IS MANDATORY. WHERE # APPEARS IN THE TABLE, THE MEASURE IS MANDATORY BUT IMPLEMENTATION MAY NOT BE POSSIBLE IMMEDIATELY DUE TO IMMATURITY OF THE TECHNOLOGY OR OTHER FACTORS. HOWEVER SUCH TECHNOLOGIES SHOULD BE FACTORED INTO UNIT STRATEGIC PLANS AND IMPLEMENTED AS SOON AS REASONABLY FEASIBLE.

Certain legal or regulatory requirements (e.g., HIPAA, PCI) may impose additional requirements beyond those listed below.

It may be possible to totally segregate networks from other parts of the network for specific purposes (e.g., a research sandbox with lesser requirements). Such instances must be coordinated with ITS Security Operations and Services.

Minimum Security Baseline Definitions

Element	Technical Requirement	Definition	Public	Non-Public (Internal/Controlled or Restricted)	Resources
CATEGORY 1 Protection from the public Internet or external network segments (direct probes)					
1.1	**The system will be segregated from direct hostile access initiated from the public Internet or network segments external to the local network**				
1.1.1	Network Hardware Firewall or Equivalent is in place	*Definition 1.1.1: Traffic should only traverse the ports that are expected. Audit firewall rules regularly. Note: using TNS Services still requires rules to be established by the department.*	X	X	TNS Firewall Services (http://www.tns.its.psu.edu/ServiceCatalog/Network/LAN/Firewall.html) Category 1 Best Practices
1.1.2	Only necessary Services for the system or network are accessible (enforced by a combination of system and/or firewall/network controls)		X	X	Category 1 Best Practices
1.1.3	DMZ or equivalent additional segregation (By segregation from public or non-local network segments by VPN, VLAN or separate network or firewall interface)			X	sos.its.psu.edu or tns.its.psu.edu Category 1 Best Practices

1.1.4	Host-based Firewall (as appropriate to the Operating System)	*Definition 1.1.4: Not all Operating Systems will currently support this requirement. This will be dependent on the performance impact and business needs - consult with Security Operations and Services.*		X	Category 1 Best Practices
1.1.5	Network Intrusion Detection System and/or Prevention System			X	Category 1 Best Practices
1.1.6	Host Intrusion Detection System, File Integrity Monitor (e.g., Tripwire) or database integrity check	*Definition 1.1.6: Application whitelisting is an option to meet this requirement.*		#	Category 1 Best Practices
CATEGORY 2: Systems connecting to the Penn State network will be remediated from known vulnerabilities					
2.1	**Systems will be remediated from known vulnerabilities upon attachment to the network**				
2.1.1	Network Access Control measures checking system health prior to connection	*Definition 2.1.1: This control is not required, but is a recommended practice.*			Category 2 Best Practices
2.1.2	Penetration testing will be conducted	*Definition 2.1.2: Security Operations and Services or a third party may be used to conduct the penetration testing. Units may be authorized to conduct their own penetration testing if the test plan is approved by Security Operations and Services.*		#	Category 2 Best Practices
2.1.3	Automatically updated Anti-Virus software (as appropriate to the Operating System)	*Definition 2.1.3: This will be dependent on the business need - consult with Security Operations and Services.*	X	X	https://downloads.its.psu.edu/ Category 2 Best Practices
2.1.4	Anti-virus software is configured to check for attempted virus introduction from multiple vectors (web, USB, etc.) in addition to boot and email virii		X	X	https://downloads.its.psu.edu/ Category 2 Best Practices

2.1.5	Automatically updated Anti-Spyware software (as appropriate to the Operating System)	*Definition 2.1.5: Some anti-virus software packages now include anti-spyware. A separate software package is not required.*	X	X	Category 2 Best Practices
2.1.6	Automatic updates are implemented for the Operating System itself. In the case of servers, there may be a limited test interval prior to update.	*Definition 2.1.6: Servers may require additional testing prior to updating; therefore, automatic updates may not be reasonable. However, testing and updates should be applied within a 30-day cycle, as critical updates are released.*	X	X	Windows Machines: ITS WSUS Server: http://ait.its.psu.edu/services/identity-access-management/ad/wsus.html Category 2 Best Practices
2.1.7	Effective and timely update processes are implemented for the applications on the system. (Automatic update where allowed by the application)	*Definition 2.1.7: This applies to applications that are hosted internally or externally, including but not limited to the Microsoft Suite.*	X	X	Category 2 Best Practices
2.2	**Systems will be checked periodically after joining the network to help ensure they do not contain known vulnerabilities**				

2.2.1	Vulnerability Scan will be conducted at regular intervals. Significant vulnerabilities will be remediated.	*Definition 2.2.1: Vulnerability Scanning is a service available through SOS-ITS that enables the University to proactively identify and remediate system vulnerabilities within the Penn State enterprise. These scans are conducted using a Tenable product named SecurityCenter. Units are permitted to use SecurityCenter for routine scans of their own network assets. This allows them to secure hosts prior to deployment and to secure existing assets against any newly identified threats. (Access to Security Center must be approved by the Unit IT/Network Manager.) Please note that self-scanning does not apply to Compliance Scans (AD19, AISGI, PCI). These must still be submitted to SOS for completion via this form: http://sos.its.psu.edu/services/vuln.html.* *This requirement applies to any device that has an IP Address in the range being scanned. There are some devices that may be excluded - please consult with Security Operations and Services.*	X	X	Vulnerability Scanning Services: http://sos.its.psu.edu/services/vuln.html Security Center is available for individual units to do this but compliance scans must be first done by Security Operations and Services. Category 2 Best Practices
2.3	**Applications made accessible over the Web will be scanned for known web application vulnerabilities**				
2.3.1	Application Assessment will be conducted by ITS for custom Web Applications	*Definition 2.3.1: The public requirement is meant to address a public site that is a portal to an internal/controlled or restricted site.*	#	X	Web Application Assessment Services: http://sos.its.psu.edu/services/webapp.html Category 2 Best Practices

2.3.2	Application Level Firewall will be implemented	*Definition 2.3.2: Web applications that are hosting restricted data must implement an application level firewall. Internal/controlled data should implement as soon as feasible. Compensating controls may satisfy this recommendation.*		#	Category 2 Best Practices
CATEGORY 3: Access to systems will be individually controlled. All actions must be traceable to a unique user id.					
3.1	**Access to multi-user systems will be individually controlled/authenticated**				
3.1.1	Strong Password Authentication	(see below)	X	X	Strong password policy (minimum length and complexity in accordance with Password Creation Guidelines: http://its.psu.edu/be-safe/password-best-practices enforced and passwords changed upon initial login Category 3 Best Practices

Definition 3.1.1: Minimum "Password" criteria are:

a. Password guidelines must be distributed to all users of the system.

b. All accounts must have passwords.

c. Passwords for accounts must not be shared, unless a Group account has been specifically authorized in writing as described in this guideline and Policy AD20. The registered user of an account must have unique access to the account because of the liability stated under Policy AD20. In those rare instances where password sharing is authorized, all individuals authorized access to the account are held jointly accountable.

d. Passwords must have at least annual expiration dates (if the operating system allows the setting of expiration dates) and it is strongly recommended that passwords be changed every three months. In some instances a shorter period (less than 90 days) is appropriate.

e. Passwords must be resistant to a computer program that checks passwords against previously used passwords and passwords that are easily discovered or compromised by human or computational means.

f. Passwords must use a mix of alpha, numeric and special characters, and contain at least 8 characters if the operating system supports passwords of that length. If not, the password should be the maximum length supported by the operating system. If passwords are not supported natively by the operating system, this requirement may be fulfilled by vendor or developed software.

g. Passwords to Computer and Network Resources containing Computerized Institutional Data will not be issued over network media in clear text unless a secondary means of authentication is provided (e.g., smart cards or tokens with one-time values, or a phone device with a similar one-time value).

3.1.2	Authentication mechanism beyond single id/password pair (e.g., challenge/response, personal image selection, grid card)	*Definition 3.1.2: This should be applied for public-facing content where a Penn State account is not required for data submission. The purpose is to limit automated abuse.*	(see definition)	# (For remote access to Internal/controlled but not Restricted data) X (Mandatory for Restricted data)	Category 3 Best Practices
3.1.3	2 Step authentication with true single use password (e.g., SecurID Token)			# X (Mandatory for Restricted data. University-wide solution underway so unit may wait to implement based on availability)	Category 3 Best Practices
3.1.4	Local Administrator Rights will generally be disallowed. Least Privilege Mode will be used, such that running as an administrator is limited to those functions that actually require administrator privileges.	*Definition 3.1.4: The definition of academic accounts will vary per department.*	X	X	Reference Least Privilege White Paper: http://sos.its.psu.edu/resources/pdfs/privileges.pdf. Elevate only when needed. Category 3 Best Practices
3.1.5	A logon banner will be displayed signifying agreement to abide by Penn State Policies. Continued use beyond the banner screen means concurrence.	*Definition 3.1.5: It is recommended that this be implemented for every logon.*	#	#	Category 3 Best Practices
3.1.6	Account access will be logged (See Category 4)		X	X	Category 3 Best Practices
3.2	**Access to personal desktop systems or laptops will be individually controlled. All actions must be traceable to a unique user.**				
3.2.1	A password is required to access any of the features of the operating system		X	X	Category 3 Best Practices
3.2.2	A logon banner will be displayed signifying agreement to abide by Penn State Policies. Continued use beyond the banner screen means concurrence.	*Definition 3.2.2: It is recommended that this be implemented for every logon.*			Category 3 Best Practices

3.2.3	Authentication mechanism beyond single id/password pair (e.g., challenge/response, personal image selection, grid card)			#	Category 3 Best Practices
3.2.4	Local Administrator Rights will generally be disallowed. Least Privilege Mode will be used, such that running as an administrator is limited to those functions that actually require administrator privileges.		X	X	Reference Least Privilege White Paper: http://sos.its.psu.edu/resources/pdfs/privileges.pdf. Elevate only when needed. Category 3 Best Practices
CATEGORY 4: Access to systems and applications (beyond public display) will be logged.					
4.1	**Access will be logged and the log record will be retained for a time interval sufficient to meet incident response and legal/regulatory requirements**				
4.1.1	System level audit logs will be retained showing both general and privileged access		X	X	Category 4 Best Practices
4.1.2	Application level audit logs will be retained showing both general and privileged access		X	X	Category 4 Best Practices
4.1.3	Network Level audit logs (e.g., firewall logs) will be retained showing both general and privileged access	*Definition 4.1.3: Logging of authentication events (successes and failures) and general and privileged network access events on systems and applications, and retention of logs as appropriate per AD35 or more stringent Federal, State or industry regulations.*		X	Category 4 Best Practices
4.1.4	At a minimum, transaction records will be retained for electronic email (date/time/IP source/to and from)	*Definition 4.1.4: Logging of transaction based events on systems such as e-mail and web servers, and retention of logs as appropriate per AD35 or more stringent Federal, State or industry regulations.*	X	X	Category 4 Best Practices

4.1.5	Audit logs will be retained for a period of time commensurate with Incident Response and legal/regulatory requirements	*Definition 4.1.5: University Policy AD35 should be consulted. Access to financial information systems requires storage for 7-years.*	Verify that audit logs are available for at least one month online and processes are in place to immediately restore at least the last years' logs for analysis.	Reference AD35	Category 4 Best Practices
CATEGORY 5: Data will be secured at rest or in transit commensurate with its sensitivity					
5.1	**Sensitive data will be encrypted wherever it resides.**				
5.1.1	Full Disk Encryption will be used to prevent recovery in the event of desktop or laptop theft (when such technology is supported by the Operating System). File Encryption for non-public files must be used in any case where full disk encryption is not possible	*Definition 5.1.1: If you use a laptop computer, your computer will need to be encrypted fully in order to be able to confirm that no data is at risk should the computer be lost or stolen. ITS will be publishing information with regard to the encryption project as soon as the project is ready for the University community. Certain work desktop computers will also be subject to encryption depending on the sensitivity of data processed and the risk of theft associated with its physical location.* *Once the drive is encrypted, there is very little impact to the user. The user may need one additional password. Hardware encryption is acceptable. A key management system is required.* *A compensating control may include the proper physical security measures.*		# (Pending license availability from SOS) X (Mandatory for Restricted data)	Encryption resources: http://sos.its.psu.edu/services/encryption.html Category 5 Best Practices

5.1.2	Individual File Encryption will be used	*Definition 5.1.2: As an alternative to Individual file encryption on a server, file- or folder-level permissions may be implemented. The purpose of this is to protect online files that are not open and in use but which reside on the hard drive of the active machine.*		#	Category 5 Best Practices
5.1.3	For server class machines that are professionally administered and physically secured, data at rest need not be encrypted. However, mechanisms must exist to prevent unauthorized disclosure of the data between user accounts and/or sessions			X (Exception to 5.1.1 and 5.1.2 for physically secured, professionally administered servers. However, 5.1.3 requirement then applies. Restricted data may have additional requirements.)	Category 5 Best Practices
5.2	**Sensitive data will be strongly encrypted when transmitted over local or wide area networks**				
5.2.1	Encrypted transmission means (e.g., TLS, SFTP, IPSec VPN) will be used wherever possible	*Definition 5.2.1: Data that is being shared with another entity, sent to an application or stored at a location must be transmitted securely using TLS, SFTP, IPSec VPN or another acceptable technology.*		X	Category 5 Best Practices
5.2.2	Sensitive communications will be encrypted	*Definition 5.2.2: Sensitive communications may include email, attachments, text, fax, etc. Compensating controls may include network segregation.*		#	Category 5 Best Practices
CATEGORY 6: Storage media that have contained sensitive data must be physically destroyed when no longer needed or sanitized prior to re-use by another entity, either internal or external to the University					
6.1	**Storage media that have contained sensitive data must be physically destroyed when no longer needed or sanitized prior to re-use by another entity, either internal or external to the University**				

6.1.1	Secure media sanitization must be used prior to transfer of equipment	*Definition 6.1.1: Secure disk and file system sanitization to be used prior to transfer of equipment (e.g., between personnel, University units, or other transfer of ownership internal or external to the University). The level of sanitization will depend on the sensitivity of information previously on the machine.*		X	Category 6 Best Practices
6.1.2	Media that have handled sensitive data must be securely destroyed when no longer needed	*Definition 6.1.2: Refer to Auxiliary and Services Procedure on Lion Surplus Operations, including Sales Store; https://guru.psu.edu/proc/BS2011.pdf. The University also has a White Bag Program available for media destruction such as CDs, DVDs, and VHS tapes containing sensitive information (http://www.green.psu.edu/psuDoing/recycling/whitebag.asp). There is also a Blue Bag Program available for paper destruction (website).*		X	Category 6 Best Practices
CATEGORY 7: Physical and facility security must be maintained.					
7.1	**Physical and facility security must be in place commensurate with the sensitivity of the data**				
7.1.1	Physically secured, locked space	*Definition 7.1.1: This applies to the main area of an office with individual cubicles or individual offices.*		X	Category 7 Best Practices
7.1.2	Employee identity proofing			X	Category 7 Best Practices
7.1.3	Surveillance cameras will be used and results routinely reviewed	*Definition 7.1.3: Results reviewed by authorized personnel.*		X (as required by AD65)	Category 7 Best Practices
CATEGORY 8: A development and risk assessment process must be in place commensurate with the sensitivity of the data					
8.1	**Units developing custom applications must have a documented design, development and test methodology**				

8.1.1	Security Review for Custom Applications at Regular Intervals During Development	*Definition 8.1.1: This applies to new applications that are being built. Existing applications should be scanned for vulnerabilities prior to the introduction of a new change to the production system. Add more explanation in the FAQ's. Security review will be less complex for public applications.*	X	X	sos.its.psu.edu
8.1.2	Configuration and change control processes must be documented	*Definition 8.1.2: Changes made to applications storing data needs to be documented. Additionally, any change to the processing, storing or use of the data or system must be documented.*	X	X	sos.its.psu.edu
8.2	**A risk assessment must be conducted for custom or major-vendor supplied applications prior to introduction as a production service**				
8.2.1	Risk Review with Business Process Owner/Unit Prior to Introduction of Major Applications (Either Custom or Vendor Supplied). Formal acceptance of any residual risk	*Definition 8.2.1: Risk Management and Security Operations and Services (SOS) must be involved in the review of major applications that are being introduced into the Penn State system. SOS will look at the application from a security perspective and Risk Management will evaluate whether the risks are acceptable. Risk Management may also need to be involved in the review of the contractual language, depending on the nature of the application. The risk review for public data will be less complex.*	X	X	sos.its.psu.edu
CATEGORY 9: Units will maintain local policies in accordance with, and augmenting, University Policy AD20 (Computer and Network Security)					
9.1	**Units must ensure that appropriate policies and procedures exist in their area commensurate with the value of computing and network resources and the data residing therein**				

9.1.1	Unit Level Policy Addressing Data Protection and Backup	*Definition 9.1.1: This policy must include a backup frequency and testing mechanisms.*	X	X	Category 9 Best Practices
9.1.2	Unit Level Policy on Change Control and Configuration Management	*Definition 9.1.2: This corresponds with item 8.1.2. Changes made to applications storing data needs to be documented. Additionally, any change to the processing, storing or use of the data or system must be documented. The unit-level policy must reflect the process of documentation and define the roles of approval required for changes that are made to the use, process or storage of data, applications or systems.*	X	X	Category 9 Best Practices
9.1.3	Unit Level Policy on Acceptable Use (Augmenting AD20)	*Definition 9.1.3: Policy AD20: http://guru.psu.edu/policies/AD20.html. Develop an internal, unit-level policy that supports AD20 and is specific to the data and acceptable use within the unit and the University. Acceptable use policies should be reviewed and accepted annually.*	X	X	Category 9 Best Practices
9.1.4	Unit Level Policy on Network Security, access control and device configuration		X	X	Category 9 Best Practices
9.1.5	Contract Statement required to be shared with Third Parties. Statement will be coordinated with the Risk Management Office.	*Definition 9.1.5: Risk Management must review contractual language for new contracts that store, use or process internal/controlled or restricted data types. Existing contacts in question should be routed to Risk Management for review and consideration of an addendum as needed.*		X	Category 9 Best Practices
CATEGORY 10: Backup and Disaster Recovery measures must be in place commensurate with the value of the computer and network resources, and the data held					

10.1	**Computer and network resources must have a documented (and tested) backup and recovery plan**				
10.1.1	A backup and restore capability for both files and full systems must exist (tested)		X	X	Tivoli: http://ait.its.psu.edu/services/storage/backup/tsm.html. Category 10 Best Practices
10.1.2	Secure offsite storage must exist sufficient to allow rapid recovery of operations in the event of a disaster	*Definition 10.1.2: Acceptable offsite storage can be in a different building location or the co-location data center.*	# If determined to be critical to have online continuously	X	Category 10 Best Practices

Future Recommendations/Considerations:

Risk mitigation for end user devices

As financially feasible, it is recommended that the end user devices be moved into a Virtual Desktop Environment and controls are appropriately applied. Authentication is coupled at the network access layer. The intention is to keep as much data off of the end-user device as possible and allow a wide variety of end-user devices.

Questions raised at the 7/29/2013 open session via Adobe Connect

Recently Updated

Minimum Security Baseline Home
a minute ago • updated by JENNIFER A STEWART • view change

MSB Category 1 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 2 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 3 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 4 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 5 Best Practice.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 6 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 7 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 9 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB Category 10 Best Practices.pdf
Feb 26, 2015 • attached by JENNIFER A STEWART

MSB FAQs
Feb 26, 2015 • created by JENNIFER A STEWART

MSB - Downloadable version 001.pdf
Dec 01, 2014 • attached by JENNIFER A STEWART

Minimum Security Baseline Home
Apr 22, 2014 • updated by RANDY L HEGARTY • view change

Minimum Security Baseline
May 06, 2013 • created by JENNIFER A STEWART

Navigate space